VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Virtuální privátní sítě, teoretický rozbor a grafická prezentace

Virtual private networks, theoretical aspects and graphical prezentation

2009 Martin Mikulec

VŠB - Technická univerzita Ostrava
Katedra telekomunikační techniky

Fakulta elektrotechniky a informatiky
Akademický rok 2008/2009

Zadání bakalářské práce

Student: **Martin Mikulec**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Virtuální privátní sítě, teoretický rozbor a grafická prezentace

Virtual private networks, theoretical aspects and graphical prezentation

Zásady pro vypracování:

V prostředí Internetu je možné přenášet citlivá data pomocí virtuálních privátních sítí.
1. Teoretický rozbor problematiky virtuálních privátních sítí.
2. Návrh a konfigurace VPN v prostředí OS Linux.
3. Grafické zpracování dané problematiky pomocí Flashe.

Seznam doporučené odborné literatury:

THOMAS, M. *Zabezpečení počítačových sítí bez předchozích znalostí.* Brno: Computer Press 2005. 338 s. ISBN 80-251-0417-6
KRČMÁŘ, P. *Linux postavte si počítačovou síť.* Praha: Grada 2008. 182 s. ISBN 978-80-247-1290-1

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Pavel Nevlud**

Datum zadání: 30.11.2008
Datum odevzdání: 07.05.2009

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * OSTRAVA *

prof. Ing. Zdeněk Diviš, CSc.
vedoucí katedry

prof. Ing. Ivo Vondrák, CSc.
děkan fakulty

Prohlášení

„Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.“

V Ostravě dne 6.května 2009 Podpis studenta ……

Abstrakt

Tato práce se zabývá problematikou propojování počítačových sítí s využitím virtuálních privátních sítí. Cílem práce je přinést přehled možností propojení dvou a více počítačových sítí a následně demonstrovat konkrétní řešení mezi dvěma směrovači.
Kapitoly první části práce uvádí do problematiky virtuálních privátních sítí, způsobů jejich vytváření a přehled o používaných technologiích a protokolech při budování virtuálních privátních sítí. Následuje kapitola, která se věnuje praktické konfiguraci virtuálního privátního tunelu mezi dvěma směrovači způsobem, aby byl každý schopen na základě této práce spojení vybudovat. Poslední kapitola je věnována grafickému zpracování problematiky vytvořením webových stránek a animací pomocí technologie flash, čímž bude práce prospěšná široké veřejnosti.

Klíčová slova

Virtuální privátní síť, enkapsulace, šifrování, utajení, integrita, autentifikace, tunelování, IPSec

Abstract

This work is dealing with problems of interconnecting computer networks using virtual private network technology. Main objective of work is bring a summary of interconnecting two and more computer networks and demonstrate practical solution between two routers. Chapters of the first part introduce overview of technologies and protocols used to establish virtual private networks. Next part is aimed to practical configuration of virtual private network between two router in way, everybody should be able to establish a connection according this quide. The last part is graphical presentation by creating a website and animation with flash technology. Presentation will be publicated for general public.

Key terms

Virtual private network, encapsulation, encryption, confidentiality, integrity, authentication, tunneling, IPSec

Seznam použitých symbolů a zkratek

ATM	Mezinárodní standart pro buňkový přenos, který zprostředkovává přenos různých typů služeb jako video nebo data v buňkách stejné velikosti 53 bytů
CE	Zákaznické rozhraní - zařízení na hraně zákazníkovy sítě
DS0	Digital signal level 0 - Specifikace rámcování používaná k přenosu digitálních signálů přes medium rychlostí 64 kb/s.
E1	přenos digitálního signálu rychlostí 2.048Mbit/s přes telefonní síť
Frame Relay	Průmyslový standart, který pracuje s různými virtuálními okruhy a používá HDLC enkapsulaci mezi připojenými zařízeními
GRE	Generic routing encapsulation - tunelovací protokol vyvinutý firmou cisco, který je schopen zapouzdřit velké množství protokolů uvnitř IP tunelu
HDLC	Bitově orientovaný synchronní protokol druhé vrstvy OSI modelu. Specifikuje zapouzdření dat na synchronních linkách používáním rámců a kontrolního součtu.
integrita	Ověření paketů, zdali nedošlo k jejich změně během přenosu
IOS	operační systém používaný ke správě zařízení firmy CISCO
IOS	Cisco operační systém, který poskytuje základní funkčnost. Je zaveden do všech produktů cisco architktury.
IP	Internetový protokol
IP datagram	Základní jednotka informace procházející přes internet
IPSec	Rozšíření IP prokolu o prvky oveření a šifrování paketů.
IPX	Přenosový protokol v síti NetWare.
ISDN	Komunikační protokol, který umožňuje telefonní síti přenášet datový či jiný provoz
ISP	poskytovatel připojení k internetu
MPLS	Multiprocol label switching - technika ke zvýšení rychlosti datového provozu.
ověření	V bezpečnosti jde o ověření identity osoby nebo procesu
PDN	veřejná datová síť
PE	rozhraní poskytovatele připojení - zařízení na hraně sítě poskytovatele připojení
PPP	Protokol bod - bod poskytuje spojení směrovač - směrovač nebo uživatel - síť přes synchronní nebo asynchronní okruhy
PSTN	Veřejná telefonní síť
SA	Prostředek k výměně informací o použitých bezpečnostních nastavením během přenosu
SHD	Synchronní diigitální hierarchie - Evropský standart, který definuje nastavení rychlosti a formátů k přenosu optických signálů přes vlákno
SONET	Synchronní optická síť fungující rychlostí až 2,5 Gbit/s
T1	přenos digitálního signálu rychlostí 1.544Mbit/s přes telefonní síť
TDM	Časový multiplex - Technika umístění několika kanálů na jedno medium
VPN	Virtuální privátní síť
X.25	ITU-T standart, který definuje, jak jsou udržována spojení mezi DTE a DCE a komunikaci mezi počítači v PDN.

Obsah

Kapitola 1

Úvod a cíl práce

V dnešní době se žádná moderní organizace neobejde bez počítačových systémů, které napomáhají jejímu chodu. K ovládání těchto systémů je třeba umožnit jejich uživatelům přístup. Proto jsou tyto počítačové systémy propojeny počítačovou sítí, která je spojuje s jejich uživateli. Velký důraz je kladen na to, aby síť byla přístupná nejen z kanceláře, ale i na cestách či z domova.

S tím souvisí celá řada výhod od finančních až po obrovskou úsporu času a zlepšení mobility pracovníků.Uživatelé v současné době očekávají plnou dostupnost síťových a internetových služeb stejně jako třeba tekoucí vodu nebo fungující elektřinu, organizace a uživatelé se stávají na těchto službách závislí a nedostupnost může způsobit vážné komplikace.

Další otázkou, kterou se síťoví správci organizace musí zabývat je způsob propojení jednotlivých poboček firmy. Jak se organizace rozrůstá do jiných lokalit, potřeba sdílení informací mezi nimi je více než žádoucí. K tomu je potřeba jednotlivé pobočky propojit, aby se chovaly jako jedna ucelená síť. Na takové spojení jsou velké nároky na spolehlivost a celkovou bezpečnost. Vzhledem k tomu, že tento problém sahá do počátků sítí, existuje celá řada řešení těchto problémů.

Ochrana dat je pro organizaci nesmírně důležitým prvkem v existenci firmy, především v její pověsti. Jako správce sítě člověk přebírá zodpovědnost za ochranu citlivých dat před zcizením a zneužitím a právě spojnice mezi pobočkami jsou zneužitelným místem.

Prudkým rozvojem internetu a rychlosti připojení k němu se naskytlo řešení pro propojení poboček přes internet pomocí tunelu. Vzhledem k nebezpečnému prostředí internetu bylo potřeba vyřešit problémy s bezpečností, jako šifrování dat, autentifikaci nebo integritu dat. Práce se tedy zabývá moderní technologií propojení poboček vytvářením virtuálních privátních sítí a cílem je přinést přehled možností propojení dvou a více počítačových sítí a následně demonstrovat konkrétní řešení mezi dvěma směrovači.

Prvním úkolem je teoretický rozbor tématu virtuálních privátních sítí, obsahuje informace o tom, co to vlastně VPN jsou, proč se v dnešní době tak rozšířilo jejich používání, informace o jejích výhodách či nevýhodách, teorii přenosu paketů, způsoby šifrování a způsoby autentizace.

V praktické části je vybudováno VPN spojení mezi směrovači. Konfigurace jednotlivých zařízení je detailně krok po kroku znázorněna a vysvětlena tak, aby byl každý schopen na základě této práce spojení vybudovat. Konfigurace je prováděna na dvou směrovačích cisco 2800 pomocí PC s operačním systémem Debian. Tyto směrovače mají v sobě integrovanou podporu virtuálních privátních sítí, PC slouží k přístupu ke konfiguraci parametrů spojení v operačním systémů cisco IOS a k ověření úspěšného propojení.

Poslední část práce poslouží široké veřejnosti k seznámení se s problematikou virtuálních privátních sítí a budou podle ni schopni si vytvořit VPN tunel mezi dvěma směrovači cisco 2800. Veřejná bude formou webových stránek umístěných na serveru školy a přiloženým cd a kromě praktické konfigurace zde bude i teoretický rozbor doplněn animacemi vytvořenými pomocí flash.

Kapitola 2

Představení VPN

2.1 Rozvoj VPN díky internetu

Problémy propojení lokálních sítí, které jsou od sebe vzdáleny, sahají do nejstarší historie sítí samotných. Donedávna se tento problém řešil pronájmem soukromých linek od některého zástupce z celé řady telekomunikačních firem, které na trhu působili. Pro mnoho firem je vytvoření spolehlivého a bezpečného spojení mezi pobočkami či obchodními partnery klíčovým faktorem v jejich podnikání. Typickým příkladem je propojení bank, jejichž zabezpečenými tunely a linkami proudí velké množství cenných dat v podobě bankovních transakcí. Nedostupnost či dokonce krádež dat na lince je považováno za zcela nepřijatelné. Totéž se dá obecně říct o každé firmě která chrání svá obchodní tajemství a další citlivé informace.

Velkou výhodou takto vytvořeného spojení byla garantovaná kvalita připojení, kterou poskytovatel zaručoval v podmínkách a také nulová starost o spojení. V případě výpadku stačilo zavolat technika, které se o problém postaral, i když čekání na vyřízení problému druhou stranou může být i nevýhodou. Postupem času došlo také ke zrychlení těchto pronajatých linek, používáním novějších technologií jako X.25, ATM nebo Frame Relay a zlepšením přenosových vlastností médií, takže bylo možno přenášet velké objemy dat na čím dál tím delší vzdálenosti.

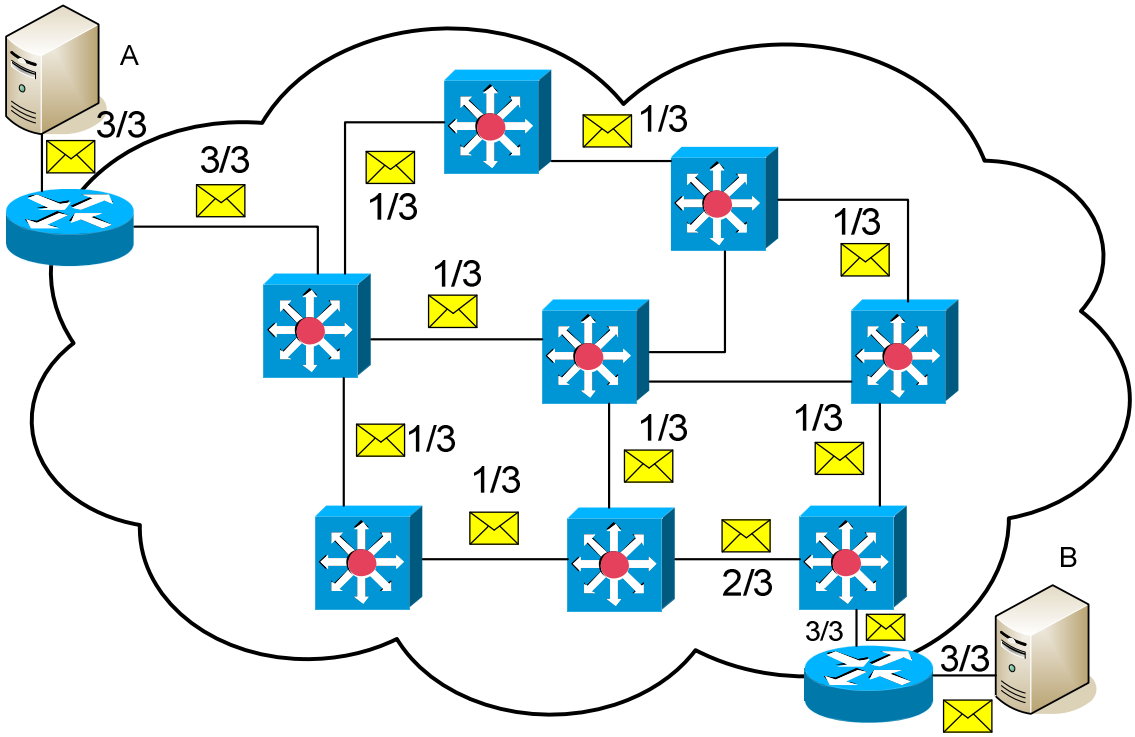
Limitem těchto technologií však byla jejich vysoká cena a to jak pořizovací tak provozní. Telekomunikační firmy si nechaly všechny nabízené služby patřičně zaplatit, takže provoz linek byl pro firmu nemalou finanční zátěží. Další nevýhodou pronajatých linek byla jejich nízká bezpečnost, která se s rozvojem internetu stala jednou ze základních otázek síťové správy, informace v digitální podobě se staly terčem nejrůznějších útoků a jejich nedotknutelnost klíčová pro existenci firmy.

Díky rozvoji internetu a zvyšování rychlosti připojení k této síti tak nastala možnost propojit sítě skrz ni. To však znamenalo celou řadu komplikací, které mohou v tomto spojení nastat.

2.2 Nevýhody a problémy VPN

Prvním, a doposud stále otevřeným, problémem je otázka garance přenosu. Internet je veřejná paketová síť, cesta paketu v ní není jednoznačně určena a není nikdo, kdo by garantoval, že paket nebude po cestě někde zahozen, že doputuje spolehlivě do cíle.

Obrázek paketové sítě



Obrázek 2.1: Příklad paketové sítě

Existují samozřejmě kontrolní mechanismy, které nám kontrolují, jestli jsou přenesená data kompletní a vyžadují části dat, které se správně nepřenesly, ale vše se projeví na době přenosu dat.

Dalším problémem je, že internet je síť veřejná, tudíž bezpečnost dat procházející touto sítí je vážně ohrožena. V dnešní době už je uskutečnění odposlechu otázkou několika kliknutí ve správném programu, proto se na bezpečnosti cestujícího paketu věnuje velká pozornost. Používá se šifrování provozu, zajišťuje se integrita dat a autentizace jednotlivých stran, které si data posílají. Žádný mechanismus nám však nezaručí, že data nebudou rozluštěna, nejmocnější šifrovací algoritmy jsou navrženy takovým způsobem, aby je nebylo možno v reálném čase za pomoci reálného výpočetního výkonu rozluštit, což zaručuje jejich praktickou nerozluštitelnost, teoreticky je to však stále možné.

Posledním problémem může být složitost konfigurace VPN spojení, která vyžaduje odborné znalosti z oblasti počítačových sítí a síťové bezpečnosti a také pořizovací cena zařízení, která umí toto spojení vybudovat. Oproti pronajatým linkách je však tato cena několikrát nižší při porovnatelném výsledku propojení.

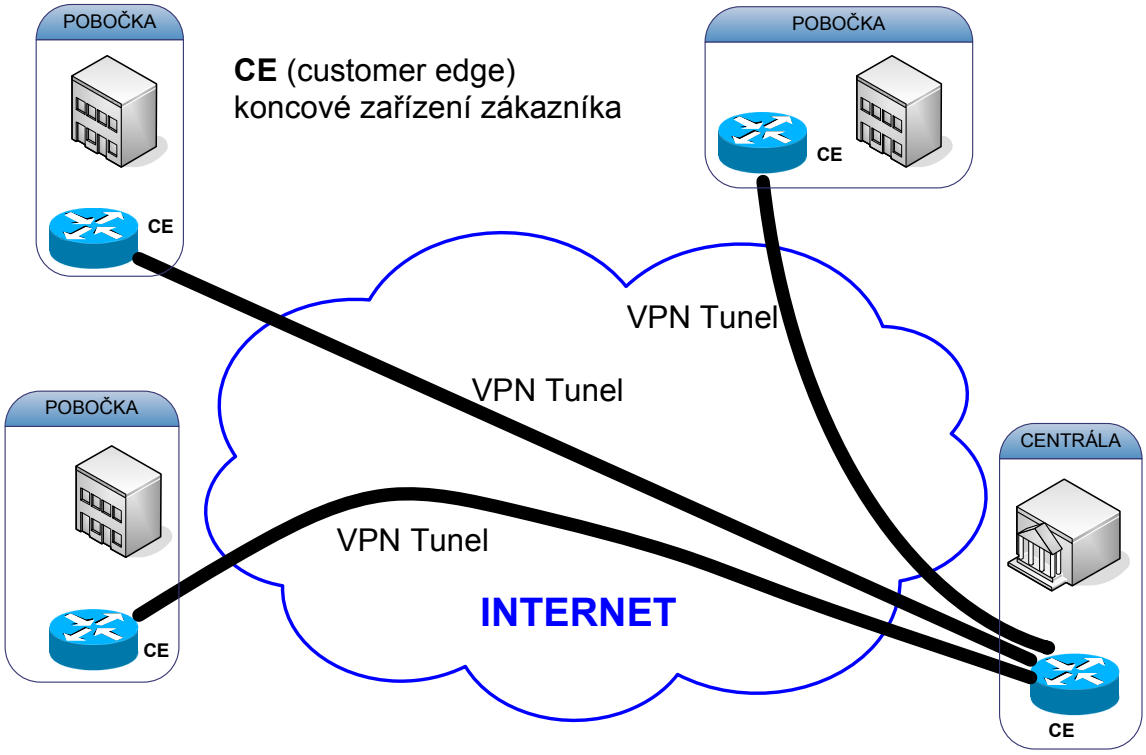
Kapitola 3

VPN spojení

3.1 Propojení síť – síť

VPN umožňuje nejen propojení bod - bod, ale lze ji kombinovat do nejrůznějších modelů. Základním rozdělením je model síť – síť (site to site) nebo vzdálený přístup.

Síť – síť umožňuje připojení mezi organizacemi působících na různých místech, obvykle bývá jedna centrála a k ní připojené pobočky.

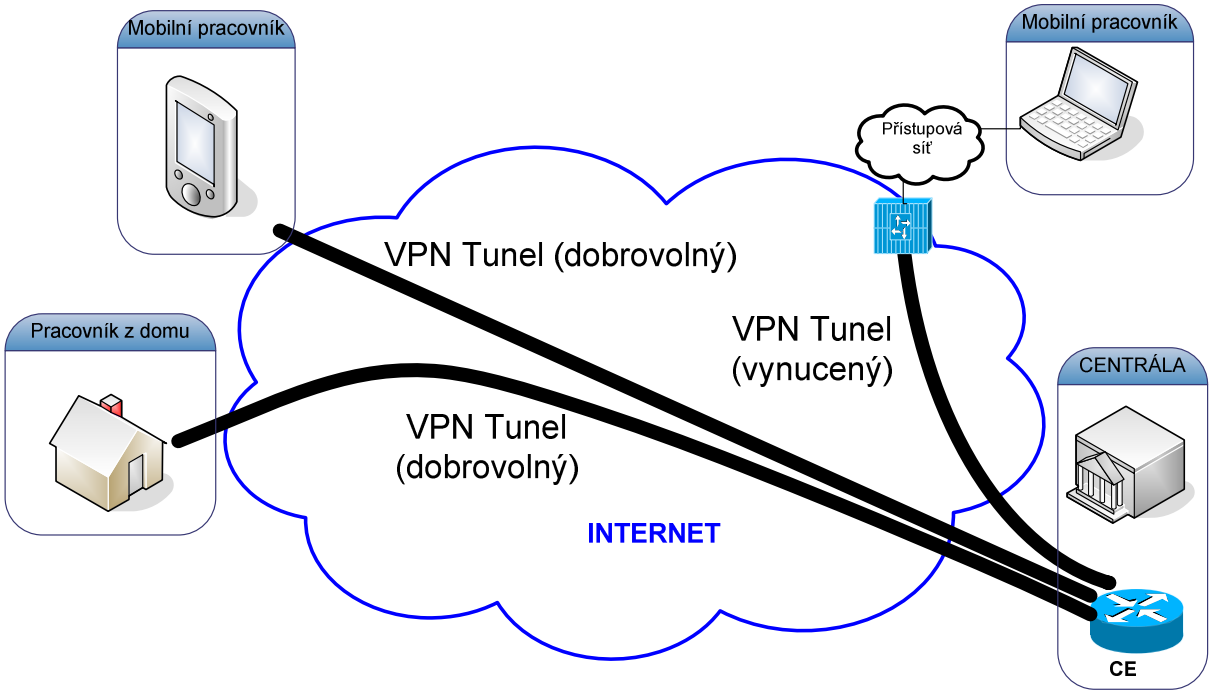


Obrázek 3.1: topologie síť - síť

Dále síť – síť VPN dělíme na intranet VPN, které umožňují propojení mezi sítěmi jedné organizace a na extranet VPN, které umožňují propojení mezi organizacemi jako obchodní partneři nebo její zákazníci.

3.2 VPN pro vzdálený přístup

VPN pro vzdálený přístup (Remote access VPN) jsou mobilní uživatelé nebo uživatelé pracující z domova, kteří používají firemní prostředky vzdáleně.



Obrázek 3.2: Tolopogie vzdálený přístup

VPN sítě se vzdáleným přístupem mohou být konfigurovány ve dvou režimech, povinném a dobrovolném tunel módu.
Povinný tunel mód je vytvářen poskytovatelem připojení. V tomto módu se vzdálený klient připojí do NAS, který tuneluje klientova data do a z VPN brány (koncentrátoru). Příkladem protokolu, který tohle umožňuje je L2F, PPTP a L2TP.

Dobrovolný tunel mód je vytvářen buď poskytovatelem připojení nebo samotným klientem.V tomto módu je datový provoz tunelován přímo mezi vzdáleným klientem a VPN bránou.

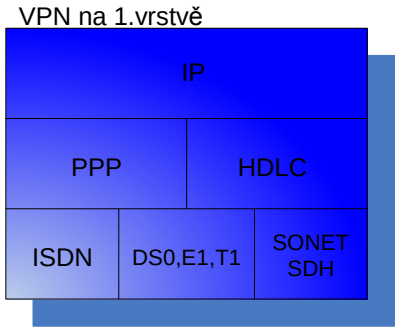
Jedním typem VPN sítě se vzdáleným přístupem je virtuální privátní vytáčená síť (Virtual Private Dialup Network), ve které se mohou vzdálení uživatelé připojit přes PSTN nebo ISDN do vytáčeného NAS. Datový provoz je poté tunelován do VPN brány.

3.3 Dělení VPN

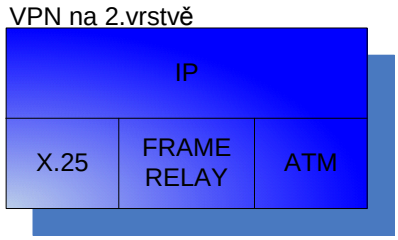
3.3.1 Podle vrstvy spojení

VPN síť – síť dělíme podle vrstev, na které jsou propojeny. Rozdělení podle vrstev je následující:

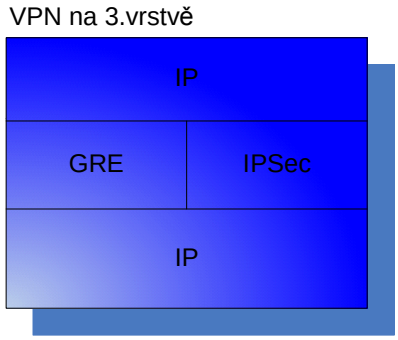
Vrstva 1 – v této vrstvě je použito tradiční časové multiplexování (TDM). Poskytovatel připojení přiřadí zákazníkovi kousek vedení a vytvoří připojení na první vrstvě mezi sítěmi zákazníka skrz ISDN, DS0, T1, E1, SONET nebo SDH a na zákazníkovi už je implementace protokolů vyšších vrstev jako PPP, HDLC nebo IP.



Vrstva 2 – VPN na druhé vrstvě je řešeno jako tradiční přepínaná WAN síť. Poskytovatel připojení je zodpovědný za vytvoření virtuálních okruhů mezi sítěmi zákazníka přes X.25. Frame Relay nebo ATM a zákazník je odpovědný za IP vrstvu a výše.



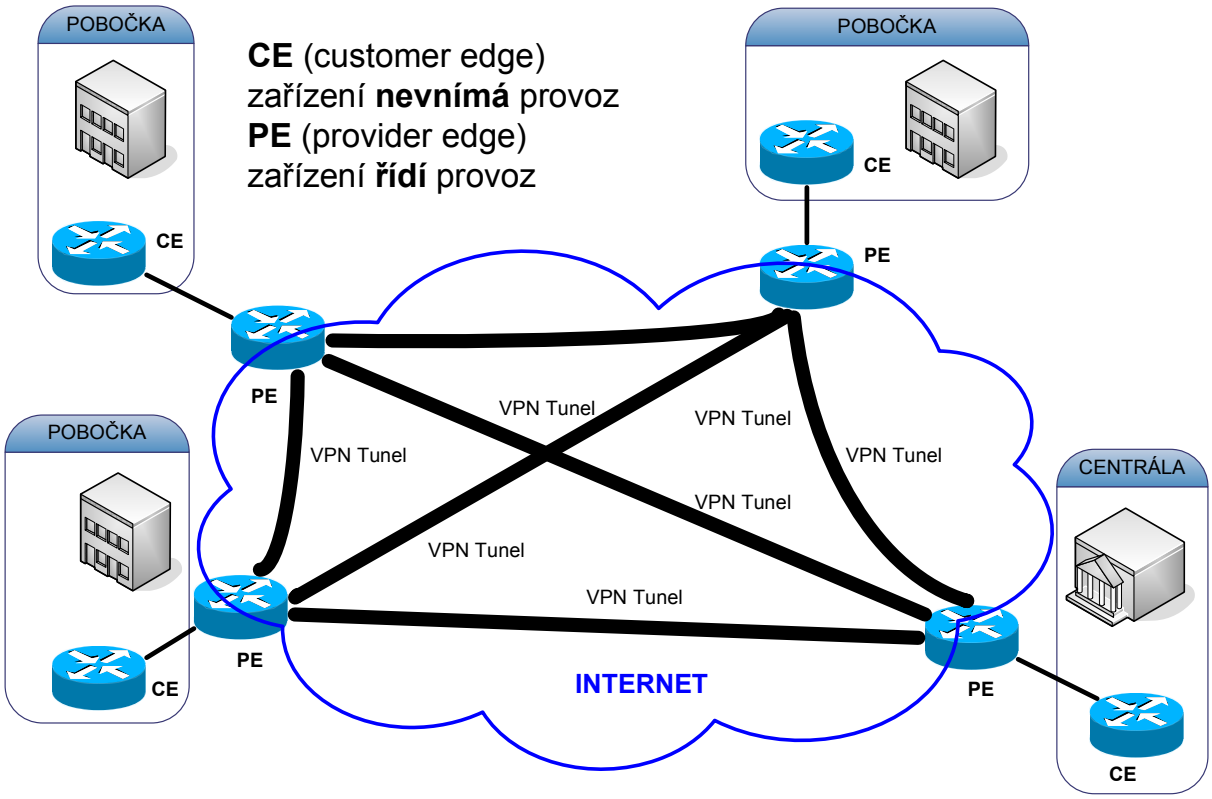
Vrstva 3 – VPN na třetí vrstvě implementováno jako bod – bod IP tunely, kde je cílové zařízení dosaženo transparentně bez toho, aby zdroj znal topologii, kterou je paket přenášen. Proto mohou být virtuální sítě vytvořeny svázáním jinak nepřipojených zařízení k sobě dohromady přes tunel. Tunely také umožňují použití privátního rozsahu napříč páteřní sítí poskytovatele připojení bez používání NAT. Tunely jsou vytvořeny použitím protokolů GRE nebo IPSec s tím, že IPSec je náročnější na zatížení procesoru zařízení, ale zato poskytuje robustnější zabezpečení.



Obrázek 3.3: VPN dle vrstev

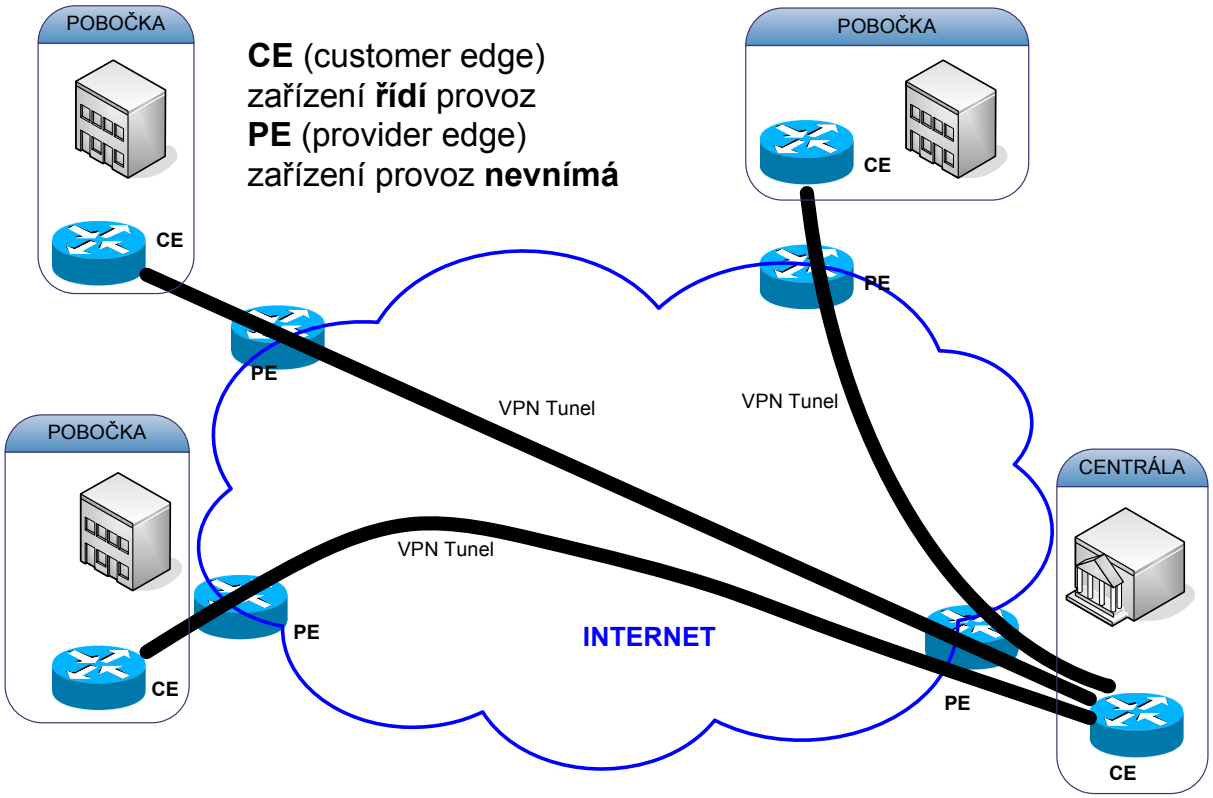
3.3.2 Podle hraničních směrovačů

PE-based VPN – PE je hraniční zařízení poskytovatele připojení a řadíme mezi ně ISP routery, přepínače nebo zařízení, která jsou kombinací obou. PE zařízení se zúčastňují směrování a přeposílání provozu na základě adresního úspořádání zákazníka. Data jsou obvykle přenášena mezi PE zařízeními přes VPN tunely vytvořených pomocí MPLS, IPSec, L2TPv3 nebo GRE. V tomto případě si CE zařízení neuvědomují že jsou součástí VPN.



Obrázek 3.4: PE based VPN

CE-based VPN – CE je hraniční zařízení zákazníka propojené s PE. PE se v tomto modu neuvědomují VPN provoz, o něj se starají CE zařízení, které provádí směrování a posílání prozovzu uživatele. Tunely jsou vytvořeny mezi těmi CE zařízeními používáním protokolů jako IPSec nebo GRE.

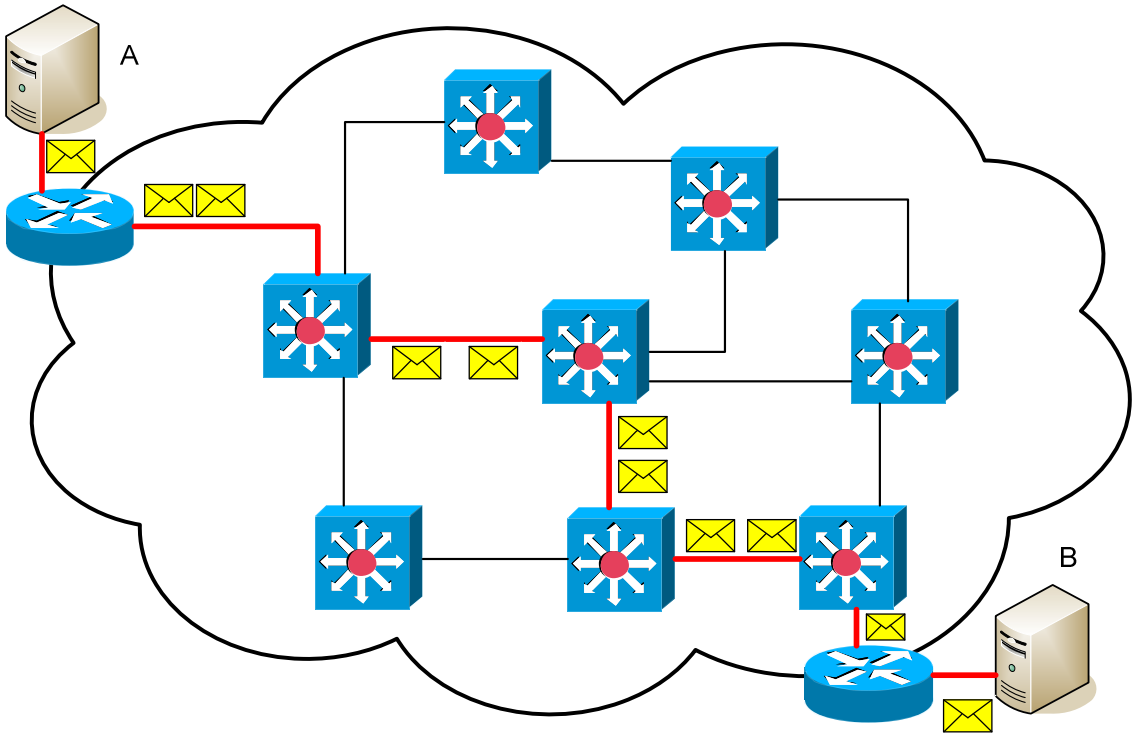


Obrázek 3.5: CE based VPN

3.3.3 Další dělení

Existuje celá řada dalšího dělení VPN sítí např. podle toho, zdali je síť spojová či bezspojová, rozprostřená či klient – klient nebo zabezpečená či důvěryhodná.

Spojová VPN (Connection-oriented) – virtuální okruhy či tunely jsou vytvořeny k přenosu VPN provozu. Příkladem spojové VPN sítě je Frame Relay nebo ATM, L2TP a IPSec tunely.



Obrázek 3.6: spojová VPN

Bezspojová VPN- ani virtuální okruhy ani tunely nejsou vytvořeny k přenosu VPN provozu. PE-based VPN sítě, které spoléhají na rozdělení provozu použitím ACL nakonfigurovaných na PE zařízeních jsou bezspojová VPN.

Rozprostřená VPN – virtuální okruhy a tunely jsou připojeny k CE zařízením. S ISP nedochází k výměně směrovacích informací, PE zařízení si neuvědomují síťový adresní prostor zákazníka. Příkladem je Frame Relay nebo ATM virtuální okruhy nebo GRE a IPSec tunely.

Klient VPN (Peer), PE zařízení se zúčastňuje směrování a posílání provozu, dochází k výměně směrovacích informací mezi PE a CE zařízeními.

Zabezpečená VPN – datový provoz klienta je mezi klienty autentizován a šifrován přes páteřní síť ISP nebo internet. Příkladem zabezpečených VPN jsou IPSec, SSL VPN, PPTP VPN zabezpečený přes MPPE a L2TP VPN zabezpečený použitím IPSec.

Kapitola 4

Bezpečnost přenosu dat

4.1 IPSec

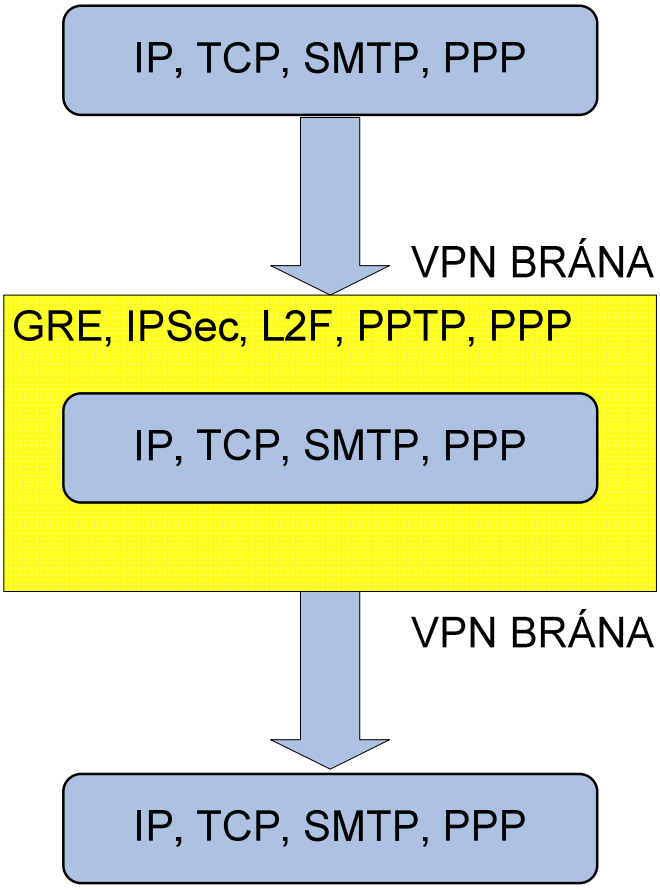
K bezpečnému přenosu dat slouží IPSec. IPSec je soustava otevřených standartů vydaná organizací Internet Engeneering Task Force (ITFT), která poskytuje řešení zachování důvěryhodnosti dat, jejich integritu a autentifikaci mezi jednotlivými členy spojení.

IPSec poskytuje tyto bezpečnostní služby na úrovni síťové vrstvy OSI modelu, užívá k tomu IKE, čímž řeší různorodost protokolů a algoritmů, které generuje šifrování a autentizační klíče použíté v IPSec. Může být nakonfigurován buď v tunel módu nebo transportním módu.

V tunel módu, celý originální IP datagram je zapouzdřen, a stává se nákladem nového IP paketu. Tento mód umožňuje síťovému zařízení pracovat jako IPSec proxy, takže zajišťuje šifrování pro všechny hosty za ním. Tyto zašifrované pakety pošle napříč IPSec tunelem. Cílový router dešifruje originální IP datagram a pošle ho do cíle.

Výhodou tunelového módu je, že chrání proti nechtěné analýze provozu, útočník je schopen rozeznat pouze koncové body spojení.
Tunelování má následují 3 základní komponenty:

- Transportní protokol, který zapouzdřujeme (AppleTalk, Banyan VINES, Connectionless Network Service [CLNS], DECnet, IP, or Internetwork Packet Exchange [IPX])
- nosný protokol – GRE nebo IPSEC protokol a ten je přenášen opět
- transportním IP protokolem.



Obrázek 4.1: Zabalení IP protokolu

V IP transportním módu je šifrován pouze náklad, originální IP hlavičky zůstávají zachovány. Výhodou tohoto módu je přidání k paketu pouze několik bytů na úkor možnosti odposlechu zdrojové a cílové IP adresy.

4.2 IKE

IKE je hybridní bezpečnostní protokol, který implementuje Oakley a SKEME výměnu klíčů uvnitř ISAKMP soustavy. IKE poskytuje autentifikaci členů spoje, vyjednává bezpečné spojení a vytváří IPSec klíče.

Konfigurace IKE je defaultně povolena na všech rozhraních routeru. Musíme tedy vytvořit IKE stanovy pro každého člena spojení. IKE stanova definuje kombinaci bezpečnostních parametrů, které jsou použity během IKE vyjednávání.

Můžeme vytvořit různé IKE (polices) stanovy, každou s různou kombinací hodnot parametrů. Pokud IKE stanovy nenakonfigurujeme, směrovač použije přednastavenou kombinaci, která je vždy nastavena na nejnižší prioritu. Pro každou stanovu nastavíme unikátní prioritu v rozmezí 1 – 10 000, priorita s hodnotou 1 je nejvyšší. Je možno nakonfigurovat různé stanovy na každého klienta, ale přinejmenším jedna z těchto stanov musí obsahovat stejné parametry použitého šifrování, hashování, autentifikace, a Diffie – Hellman hodnoty jako u vzdáleného připojeného člena. Při nezadání parametru je opět použit přednastavený.

IKE používá UDP protokol na portu 500. IPSec ESP a AH protokoly užívají IP protokol na portech 50 a 51. Častým problémem je blokace těchto portů firewallem nebo access-listy na routrech.

Při konfiguraci IPSec narazíme na celou řadu nastavení, jedním z nich můžou být šifrovací access listy používané k definování, který IP provoz bude chráněn šifrováním a který ne. Tyto access listy nejsou totéž jako klasické access listy, které vytvářejí pravidla, který provoz bude blokován či povolen.

Šifrovací access listy nejsou samy o sobě specifikovány pro IPSec. Ty jsou přiřazeny k rozhraním na základě čísla access listu.

4.3 Kryptografické mapy

Kryptografické mapy – Vzdálená zařízení potřebují být spravována skrz VPN z centrální sítě, pokud operují v centralizovaném IT modelu.VPN zařízení podporují celou řadu nejrůznějších konfigurací k nastavení koncových bodů tunelu a v závislosti na zvolené metodě mají tyto nastavení vliv na ovladatelnost sítě.

K nejefektivnější správě vzdálených zařízení je nutno použít statické kryptografické mapy v síti, kde jsou umístěny aplikace pro správu sítě.
Dynamické kryptografické mapy se používají z důvodu jednoduché konfigurace. Dynamické mapy totiž akceptují pouze příchozí IKE požadavky. Jelikož nejsou schopny požadavky vytvářet, není zaručeno, že tunel mezi zařízeními existuje.

Statické kryptografické mapy používají statické IP adresy vzdálených zařízení, tudíž i vzdálená zařízení musí používat statické IP adresy.
Pro úspěšné vytvoření IP tunelu musí být na obou stranách kompatibilní nastavení kryptografických map.

Jestliže se dvě zařízení rozhodnou uskutečnit vzájemné bezpečnostní spojení (SA), musí mít nejméně jeden záznam kryptografické mapy kompatibilní se záznamem protější strany.
Pokud mají být kryptografické mapy kompatibilní, musí splňovat následující minimální kritéria:

- Záznamy kryptografické mapy musí obsahovat kompatibilní kryptografické access listy
- Záznamy kryptografické mapy musí identifikovat přidruženého vzdáleného člena.
- Záznamy kryptografické mapy musí mít nejméně jeden transform set

4.4 Security Association

Podstatnou částí IPsec je *Security Association* neboli SA. Nastavení SA určuje úroveň důvěry mezi komunikujícími stranami. Je vytvořen logický jednosměrný kanál, kterým jsou koncová zařízení domluvena na pravidlech používaných pro přenos dat. Identifikace tohoto kanálu je jednoznačná pomocí zdrojové IP adresy kanálu, druhu použitého protokolu (ESP nebo AH) a *Security Parameter Index* (SPI). SPI je pak položkou AH i ESP hlaviček a umožňuje přiřazení příchozího paketu konkrétnímu SA kanálu a použití jeho parametrů pro zpracování paketu. Parametry SA kanálu jsou doba jeho trvání, používané algoritmy,šifrovací klíče a to zda je používán tunelovací nebo transportní mód. Vzhledem k tomu, že je SA jednosměrným kanálem, je pro obousměrnou komunikaci nutné vytvořit SA kanály dva.
Sestavení SA kanálů je možno provádět ručně nastavením jejich parametrů na obou koncích spojení. Tento způsob obvykle vyžaduje i zabezpečené přenesení klíčů mezi oběma stranami. Zcela běžnou potřebou však je pravidelná obměna klíčů. Z tohoto pohledu je manuální sestavování SA nevhodné a totéž platí i v případě správy většího počtu SA. V praxi se používá automatizovaného sestavení a správy SA za pomoci protokolu IKE *(Internet Key Exchange)* pro výměnu klíčů. Před vytvořením IPsec SA kanálu proběhne sestavení IKE vazby mezi komunikujícími stranami a následně výměna klíčů. Zásadním prvkem procesu sestavení IKE vazby je vzájemné ověření obou stran například pomocí sdíleného klíče nebo certifikátů.

4.5 Šifrování

Jestliže je běžný text posílán přes internet, může být odchycen a přečten. K zachování dat v soukromí je potřeba je šifrovat. VPN šifrování přemění data do podoby nečitelné pro neautorizované příjemce.

Šifrování funguje tak, že jako vysílač tak přijímač znají pravidla k přeměně původní zprávy do zakódované formy, znají algoritmus a klíč.
Algoritmus je matematická funkce, která kombinuje zprávu, text, číslice nebo všechno dohromady s klíčem.

Výstupem je nečitelný řetězec znaků. Rozšifrování je extrémně obtížné, ne-li nemožné bez správného klíče.

Přehledem několik způsobů šifrování.

- AH – autentifikační hlavička. – Tato hlavička, poté co je přidána do IP datagramu zajišťuje integritu a autentifikaci dat. Neposkytuje však utajení dat.
- ESP – encapsulating security payload – tato hlavička nám, pokud ji přidáme do IP datagramu, zajistí utajení, integritu a autenticitu dat

Stupeň zabezpečení poskytovaný šifrovacími algoritmy závisí na délce klíče. Čím kratší délka klíče, tím větší je šance a menší výpočetní výkon k prolomení kryptování. Mezi nejpoužívanější šifrovací algoritmy patří

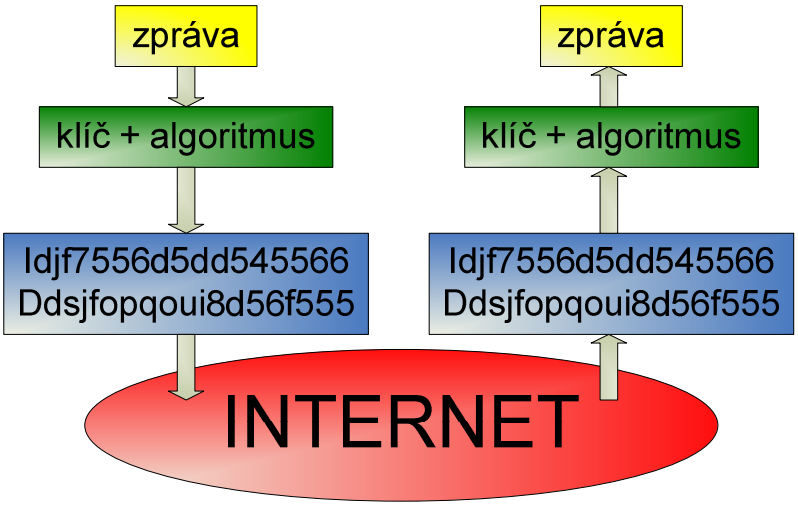
- DES – Data Encryption Standard – vynalezen firmou IBM, používá 56-bitovou délku klíče, symetrický
- 3DES - Triple DES – novější varianta
- AES – Advanced Encryption Standard – poskytuje silnější kryptování než DES a 3DES, nabízí 3 různé délky klíče 128,192 a 256-bitové.
- RSA – Rivest, Shamir and Adlesman – Klíče používají délku 512, 768, 1024 nebo více bitů. Asymetrický (jiný klíč pro šifrování a dešifrování)

4.6 Hashování

Hashovací algoritmus (Transform set) – musí být definován bez ohledu na tunelovací protokol, který používáme. Velkou roli zde hraje integrita dat

Hash, zajišťující integritu dat, je číslo generováno z řetězce textu. Hash je menší než samotný text a je generován na základě prvočísel, které je obtížné rozluštit. Vysílač vygeneruje hash ze zprávy a pošle ji se samotnou zprávou. Příjemce dešifruje zprávu a hash, vygeneruje vlastní hash z přijaté zprávy a pokud se hashe shodují, může si být jistý, že zpráva nebyla pozměněna.

VPN používá HMAC (hashed message authentication code**)** algoritmus, který garantuje integritu dat, HMAC má 2 parametry, zprávu a tajný klíč známý pouze vysílači a přijímači. Tento klíč si musí nějakou bezpečnou cestou předat.
Mezi nejpoužívanější patří
MD5 – Message Digest 5 – používá 128-bitový sdílený klíč. Výstupem kombinace zpráva + klíč je 128-bitový hash. Ten je přiřazen zprávě a poslán příjemci.
SHA-1 – Secure Hash Algorithm 1, – používá 160.bitový tajný klíč. Výstupem kombinace zpráva + klíč je 160-bitový hash. Ten je přiřazen zprávě a poslán příjemci.



Obrázek 4.2: Hashování

Kapitola 5

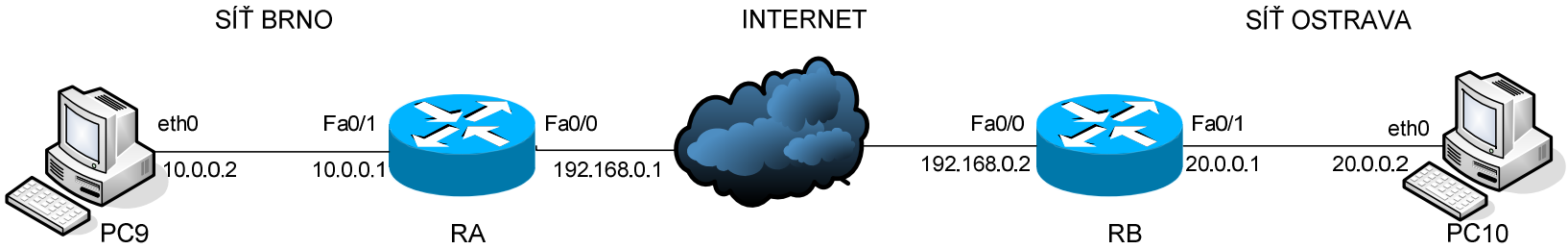
Praktická konfigurace VPN spojení

V následující kapitole přistoupíme k praktickému použití VPN technologie. Představme si fiktivní firmu, nazveme si ji například TUNELY a.s. Firma má za sebou druhý rok úspěšného startu na trhu, sídlo firmy je v Brně a díky výhodné zakázce se rozhodne rozšířit svoji působnost do Ostravy. Založí si zde jen menší obchodní pobočku s několika zaměstnanci v kanceláři a podpůrným pracovištěm pro mobilní pracovníky - obchodní zástupce, kteří využívají ke své práci různé síťové služby od tiskárny až po sdílení souborů na firemním serveru v Brně.

Po vybudování lokální sítě s hraničním routerem RB se firma zajímá, jakým způsobem zpřístupnit ostravské pobočce informace nacházející se v centrální síti v Brně. Firma už má rozpracovanou celou řadu vnitřních systémů, jak účetních, tak informačních, které je nutno sdílet zaměstnanci jak v Brně tak Ostravě. Vzhledem k nízkým nárokům na přenosovou rychlost a garanci přenosu volí firma jako nejvhodnější řešení vytvořit VPN tunel přes internet vytvořený konfigurací routerů CISCO 2800, které mají VPN řešení implementovány v sobě.

K vytvoření spojení bude tedy firma potřebovat 2 hraniční routery cisco 2800, které budou do internetu připojeny přes ISP dostatečnou přenosovou rychlostí, která bude mít vliv i na přenosovou rychlost uvnitř VPN tunelu. Na přenosovou rychlost má kromě rychlosti připojení vliv celá řada dalších aspektů. Bude záležet na výpočetním výkonu obou routerů, které budou mít s VPN tunelem mnoho práce navíc. Kromě běžného směrovaní provozu budou muset každý paket pečlivě zabalit a umístit do VPN tunelu, na opačné straně provést autentizaci, dešifrování a přeposlání a správné rozhraní do správné sítě.Tyto modely mají VPN implementovány do vnitřního operačního systému IOS.

Možností jak nakonfigurovat router je několik. Nejjednodušším připojením k němu je připojení konzolovým kabelem, který je na straně routeru připojen do správného konzolového portu. Na straně počítače obvykle vstupuje do seriového portu či portu USB. Po nakonfigurování se lze připojit i použitím telnetu či ssh. Firma ke konfiguraci používá právě konzolový port a provoz na lince si zobrazuje pomocí programu minicom, který je běžnou součástí všech linuxových distribucí a plně postačuje ke kompletní konfiguraci zařízení. Reálnou situaci si budeme simulovat následujícím rozložením prvků ve schématu:



Obrázek 5.1: Schéma zapojení

Zařízení	Rozhraní	IP adresa	Operační systém	Popis
PC9	eth0	10.0.0.2	Debian	Koncová stanice síť Brno
RA	FastEthernet 0/1	10.0.0.1	CISCO IOS	Hraniční router síť Brno, rozhraní dovnitř sítě
RA	FastEthernet 0/0	192.168.0.1	CISCO IOS	Hraniční router síť Brno, rozhraní ven ze sítě
RB	FastEthernet 0/0	192.168.0.2	CISCO IOS	Hraniční router síť Ostrava, rozhraní ve ze sítě
RB	Fastethernet 0/1	20.0.0.1	CISCO IOS	Hraniční router síť Ostrava, rozhraní dovnitř sítě
PC10	eth0	20.0.0.2	Debian	Koncová stanice síť Ostrava

Obrázek 5.2: Adresování zapojení

5.1 Konfigurace PC9

Otevřeme si okno terminálů a do něj napíšeme následující příkaz, který nám nastaví ip adresu rozhraní eth0 na hodnotu 10.0.0.2 s maskou 255.255.255.0 což odpovídá zkrácenému zápisu 10.0.0.2/24. Při nastavení musíme být v superuživatelském režimu, do kterého se dostaneme příkazem su a zadáním rootovského hesla.

```
su
ifconfig eth0 10.0.0.2 netmask  255.255.255.0
```

K tomu, aby PC věděl, kam posílat provoz je potřeba nastavit mu defaultní bránu. Defaultní bránou k PC9 je RA, konkrétně jeho rozhraní FastEthernet 0/1 s IP adresou 10.0.0.1/24. Nastavení provedeme následujícím příkazem:

```
route add default gw 10.0.0.1
```

Tím končí konfigurace PC9, nadále ho však budeme používat ke konfiguraci routeru RA.

5.2 Konfigurace RA

Otevřeme si program minicom zadáním jeho názvu do příkazové řádky terminálu, avšak k příkazu přidáme ještě příponu – s abychom se dostali do konfiguračního režimu minicomu a nastavili zde parametry pro použití seriové linky. Nastavení komunikačních paramerů portu je 9600 8N1

Bps	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Po nastavení spustíme minicom, po určité chvíli se nám ukáže na novém řádku

```
Router>
```

Přejdeme do privilegovaného módu

```
Router>enable
```

Přejdeme do konfiguračního módu

```
Router#configure terminal
```

Přejmenujeme si router na RA

```
Router#hostname RA
```

Od této chvíle máme máme router přejmenovaný a pustíme se do konfigurace jednotlivých rozhraní, ke kterým jsou připojeny další prvky.

```
RA #interface FastEthernet 0/1
```

Nastavíme IP adresu rozhraní

```
RA (config-if)#ip address 10.0.0.1 255.255.255.0
```

Rozhraní aktivujeme

```
RA (config-if)#no shutdown
```

A důkladně popíšeme

```
RA (config-if)#description link to PC9
```

Opustíme interface FastEthernet 0/1 , nakonfigurujeme FastEthernet 0/0

```
RA(config-if)#exit
```

```
RA#interface FastEthernet 0/0
```

Nastavíme IP adresu rozhraní

```
RA(config-if)#ip address 192.168.0.1 255.255.255.0
```

Rozhraní aktivujeme

```
RA(config-if)#no shutdown
```

A důkladně popíšeme

```
RA(config-if)#description link to RB
```

Předtím, než se pustíme do konfigurace RB, musíme ještě nastavit směrování do sítě 20.0.0.0/24, která není přímo připojena k routeru. Provedeme konfiguraci statického směrování:

```
RA(config)#ip route 20.0.0.0 255.255.255.0 192.168.0.2
```

5.3 Konfigurace RB

Po připojení konzolového kabelu spustíme minicom, po určité chvíli se nám ukáže na novém řádku

```
Router>
```

Přejdeme do privilegovaného módu

```
Router>enable
```

Přejdeme do konfiguračního módu

```
Router#configure terminal
```

Přejmenujeme si router na RB

```
Router#hostname RB
```

Od této chvíle máme máme router přejmenovaný a pustíme se do konfigurace jednotlivých rozhraní, ke kterým jsou připojeny další prvky.

```
RB #interface FastEthernet 0/1
```

Nastavíme IP adresu rozhraní

```
RB (config-if)#ip address 20.0.0.1 255.255.255.0
```

Rozhraní aktivujeme

```
RB (config-if)#no shutdown
```

A důkladně popíšeme

```
RB (config-if)#description link to PC10
```

Opustíme interface FastEthernet 0/1 , nakonfigurujeme FastEthernet 0/0

```
RB(config-if)#exit

RB#interface FastEthernet 0/0
```

Nastavíme IP adresu rozhraní

```
RB(config-if)#ip address 192.168.0.2 255.255.255.0
```

Rozhraní aktivujeme

```
RB(config-if)#no shutdown
```

A důkladně popíšeme

```
RB(config-if)#description link to RA
```

Předtím, než se pustíme do konfigurace PC10, musíme ještě nastavit směrování do sítě 10.0.0.0/24, která není přímo připojena k routeru. Provedeme konfiguraci statického směrování:

```
RA(config)#ip route 10.0.0.0 255.255.255.0 192.168.0.1
```

5.4 Konfigurace PC10

Otevřeme si okno terminálu na PC10 a do něj napíšeme následující příkaz, který nám nastaví ip adresu rozhraní eth0 na hodnotu 20.0.0.2 s maskou 255.255.255.0 což odpovídá zkrácenému zápisu 20.0.0.2/24. Při nastavení musíme být v superuživatelském režimu, do kterého se dostaneme příkazem su a zadáním rootovského hesla.

```
su
ifconfig eth0 20.0.0.2 netmask  255.255.255.0
```

K tomu, aby PC vědel, kam posílat provoz je potřeba nastavit mu defaultní bránu. Defaultní bránou k PC10 je RB, konkrétně jeho rozhraní FastEthernet 0/1 s IP adresou 20.0.0.1/24. Nastavení provedeme následujícím příkazem:

```
route add default gw 20.0.0.1
```

V tuto chvíli bychom měli být schopni ověřit konektivitu mezi PC9 a PC10 příkazem z PC10

```
ping 10.0.0.2
```

Pokud nám pakety prochází, vše je v pořádku a můžeme postupovat dále v konfiguraci.

5.5 Konfigurace IPSec

Přistoupíme ke konfiguraci IKE stanov na routeru RB

V konfiguračním modu vytvoříme novou IKE stanovu

```
RB(config)#crypto isakmp policy 1
```

Nastavíme autentizační metodu na pre-share – sdílení stejného klíče oběma stranami

```
RB(config-isakmp)#authentication pre-share
```

Nastavíme použité šifrování na 56-bitové DES šifrování

```
RB(config-isakmp)#encryption des
```

Nastavíme hash algoritmus na SHA Secure Hash Algorithm

```
RB(config-isakmp)#hash sha
```

Nastavíme 768-bitový Diffie-Hellman

```
RB(config-isakmp)#group 1
```

Poslední hodnotou je lifetime – čas bezpečnostní asociace, nastavíme 1 den

```
RB(config-isakmp)#lifetime 86400
RB(config-isakmp)#exit
```

Vytvoříme si sdílený klíč přiřazen ke vzdálenému členu. Prvním příkazem rozpoznání identity člena na základě jeho ip adresy.

```
RB(config)#crypto isakmp key identity address
RB(config)#crypto isakmp key test12345 address 192.168.0.1
```

Nyní si vytvoříme access list, ve kterém specifikujeme, který provoz bude šifrován a který ne

```
RB(config)#access-list 101 permit ip host 20.0.0.2 host 10.0.0.2
```

Nastavíme transform set

```
RB(config)#crypto ipsec transform-set tunel esp-aes esp-sha-hmac
RB(cg-crypto-trans)# mode tunel
RB(cg-crypto-trans)# mode exit
```

Pokračujeme konfigurací kryptografických map, nastavíme její název a sekvenční číslo

```
RB(config)#crypto map cmap 10 ipsec-isakmp
```

Nastavíme vzdáleného klienta

```
RB(config-crypto map)#set peer 192.168.0.1
```

Přiřadíme transform set

```
RB(config-crypto map)#set transform-set tunel
```

Přiřadíme vytvořený kryptografický access list

```
RB(config-crypto map)#match address 101

RB(config-crypto map)#exit
```

Přiřadíme kryptografickou mapu správnému rozhraní routeru

```
RB(config)#interface FastEthernet 0/0

RB(config-if)#crypto map cmap

RB(config-if)#exit
```

V privilegovaném režimu zkontrolujeme nastavení kryptografické mapy

```
RB(config)exit

RB# show crypto map interface FastEthernet 0/0

Crypto Map "cmap" 2 ipsec-isakmp
Peer = 192.168.0.1
Extended IP access list 101
access-list 101 permit ip host 20.0.0.2 host 10.0.0.2
Current peer:192.168.0.1
Security association lifetime:4608000 kilobytes/1000 seconds
PFS (Y/N):N
Transform sets={ tunel, }

RB# show crypto ipsec transform-set
Transform set tunel: { esp-aes esp-sha-hmac }
will negotiate = { Tunnel, },
},
```

Tím je konfigurace RB skončena, zbývá nám uskutečnit podobnou konfiguraci na RA

V konfiguračním modu vytvoříme novou IKE stanovu

```
RA(config)#crypto isakmp policy 1
```

Nastavíme autentizační metodu na pre-share – sdílení stejného klíče oběma stranami

```
RA(config-isakmp)#authentication pre-share
```

Nastavíme použité šifrování na 56-bitové DES šifrování

```
RA(config-isakmp)#encryption des
```

Nastavíme hash algoritmus na SHA Secure Hash Algorithm

```
RA(config-isakmp)#hash sha
```

Nastavíme 768-bitový Diffie-Hellman

```
RA(config-isakmp)#group 1
```

Poslední hodnotou je lifetime – čas bezpečnostní asociace, nastavíme 1 den

```
RA(config-isakmp)#lifetime 86400
RA(config-isakmp)#exit
```

Vytvoříme si sdílený klíč přiřazen ke vzdálenému členu. Prvním příkazem rozpoznání identity člena na základě jeho ip adresy.

```
RA(config)#crypto isakmp key identity address
RA(config)#crypto isakmp key test12345 address 192.168.0.2
```

Nyní si vytvoříme access list, ve kterém specifikujeme, který provoz bude šifrován a který ne

```
RA(config)#access-list 101 permit ip host 10.0.0.2 host 20.0.0.2
```

Nastavíme transform set

```
RA(config)#crypto ipsec transform-set tunel esp-aes esp-sha-hmac
RA(cg-crypto-trans)# mode tunel
RA(cg-crypto-trans)# mode exit
```

Pokračujeme konfigurací kryptografických map, nastavíme její název a sekvenční číslo

```
RA(config)#crypto map cmap 10 ipsec-isakmp
```

Nastavíme vzdáleného klienta

```
RA(config-crypto map)#set peer 192.168.0.2
```

Přiřadíme transform set

```
RA(config-crypto map)#set transform-set tunel
```

Přiřadíme vytvořený kryptografický access list

```
RA(config-crypto map)#match address 101

RA(config-crypto map)#exit
```

Přiřadíme kryptografickou mapu správnému rozhraní routeru

```
RA(config)#interface FastEthernet 0/0

RA(config-if)#crypto map cmap

RA(config-if)#exit
```

V privilegovaném režimu zkontrolujeme nastavení kryptografické mapy

```
RA(config)exit

RA# show crypto map interface FastEthernet 0/0

Crypto Map "cmap" 2 ipsec-isakmp
Peer = 192.168.0.2
Extended IP access list 101
access-list 101 permit ip host 10.0.0.2 host 20.0.0.2
Current peer:192.168.0.2
Security association lifetime:4608000 kilobytes/1000 seconds
PFS (Y/N):N
Transform sets={ tunel, }

RA# show crypto ipsec transform-set
Transform set tunel: { esp-aes esp-sha-hmac }
will negotiate = { Tunnel, },
},
```

Z PC9 ověříme fungující VPN propojení

```
ping 20.0.0.1
```

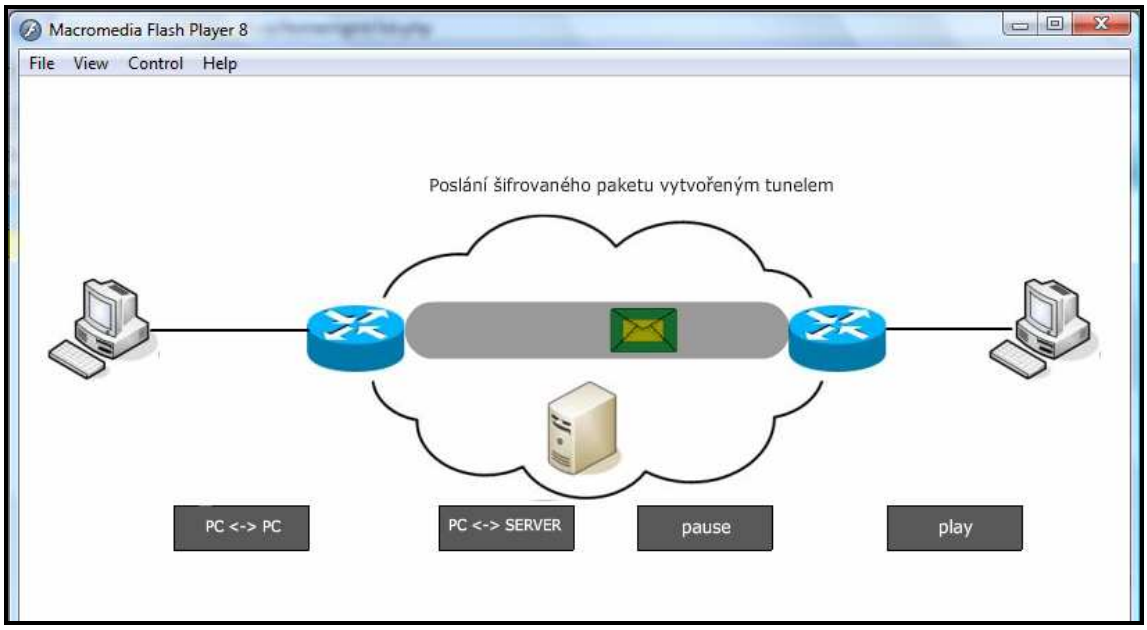
Kapitola 6

Grafická prezentace

K bakalářské práci je vytvořena grafická prezentace, která se stane návodem pro studenty počítačových sítí. Webová prezentace je umístěna veřejně na serveru školy na adrese http://homel.vsb.cz/~mik560/vpn a obsahuje jak teoretické informace obsažené v prvních kapitolách, které studentovi pomůžou zorientovat se v problematice, tak i praktickou konfiguraci VPN tunelu mezi dvěma směrovači CISCO 2800. Součástí konfigurace je i přehledné schéma, ze kterého jsou patrné možnosti, které má při konfiguraci jednotlivých parametrů spojení.

Pro lepší pochopení problematiky byla vytvořena animace, která znázorňuje cestu paketu sítí a budování VPN tunelu mezi směrovači.

Obrázek 6.1: Webová prezentace



Obrázek 6.2: Animace

Kapitola 7

Závěr

Cílem této práce je vypracovat podklady pro výuku, který budou využity ve cvičení počítačových sítí, konkrétně problematiku VPN spojení. Obsahuje nezbytné informace, které při budování VPN spojení bude potřeba. V teoretické části se nachází popis, jaké topologie a protokoly se běžně používají, a také vysvětlení termínů, se kterými se je možno se setkat při praktické konfiguraci VPN jako IPSec, IKE, kryptografické mapy, security association, šifrovací a hashovací algoritmy.

V praktické části se nachází podrobný návod na konfiguraci VPN tunelu mezi dvěma směrovači CISCO 2800 a podrobné schéma, kterým je možno se řídit při konfiguraci.

Všechny tyto informace jsou také veřejně dostupné v podobě webové prezentace umístěné na serveru školy na adrese http://homel.vsb.cz/~mik560/vpn i v příloze a obsahuje navíc i animaci, která znázorňuje putování paketu sítí a tvorbu VPN tunelu.

Do budoucna může být projekt rozvíjen mnoha dalšími konfiguracemi a vytvořit tak kvalitní podklad pro výuku počítačových sítí.

Kapitola 8

Použitá literatura

[1] *Site-to-Site and Extranet VPN Business Scenarios* [online]. [1992-2009] [cit. 2009-05-02]. Dostupný z WWW: <http://www.cisco.com/en/US/docs/security/vpn_modules/6342/configuration/guide/6342site3.html#wp1035810>.

[2] *Dynamic LAN-to-LAN VPN between Cisco IOS Routers* [online]. [1992-2009] [cit. 2009-05-02]. Dostupný z WWW: <http://www.cisco.com/en/US/docs/security/vpn_modules/6342/configuration/guide/6342vpn4.html>.

[3] LEWIS, Mark. The ABCs of VPNs. Packet magazine [online]. 2006, vol. 18, no. 2 [cit. 2009-02-28]. Dostupný z WWW: <http://www.cisco.com/web/about/ac123/ac114/downloads/packet/pdf/PK182.pdf>.

[4] NAM-KEE, Tan. Building VPNs : with IPSec and MPLS. 1st edition. [s.l.] : McGraw-Hill, 2003. Dostupný z WWW:

<http://searchnetworking.techtarget.com/searchNetworking/downloads/Buildvpn1.pdf>. ISBN 0071409319. The VPN Overview

[5] LEWIS, Mark. Comparing, Designing, and Deploying VPNs. 1st edition. Indianapolis (USA) : Cisco Press, 2006. Dostupný z WWW: <http://www.ciscopress.com/content/images/1587051796/samplechapter/1587051796content.pdf>. ISBN 1-58705-179-6. What Is a Virtual Private Network?.

[6] CARMOUCHE, James Henry. IPsec Virtual Private Network Fundamentals. 1st edition. [s.l.] : Cisco Press, 2006. Dostupný z WWW: http://www.ciscopress.com/content/images/1587052075/samplechapter/1587052075_ch03.pdf. ISBN 1-58705-207-5. Chapter3 : Basic IPsec VPN Topologies and Configurations,

[7] *Cisco curriculum CCNA4 : chapter 6.3* [online]. c2007-2009 [cit. 2009-05-02]. Dostupný z WWW: <http://curriculum.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/SESSION_ID=1241270139423990,LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=en,Version=1,RootID=knet-lcms_exploration4_en_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/theme/cheetah.html?cid=1400000000&l1=en&l2=none&chapter=6>. Access only Cisco network academy students.

Přílohy

obsah CD

složka www obsahuje webovou prezentci

složka flash obsahuje zdrojový kod flash.fla animace i animaci flash.swf

složka literatura obsahuje dokumenty použité při psaní

- 1587051796content.pdf
- 1587052075_ch03.pdf
- Build VPN.pdf
- magazin.pdf

složka bp obsahuje bakalářskou práci

- bakalářská_práce_mik560.pdf